PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-139701
(43)Date of publication of application : 31.05.1996

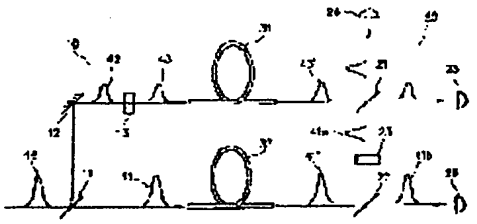
(51)Int.Cl. H04K 1/00

(21)Application number : 06-280449
(22)Date of filing : 15.11.1994

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : IMOTO NOBUYUKI

(54) QUANTUM CIPHER SYSTEM

(57)Abstract:
PURPOSE: To provide a quantum cipher system which has high tapping detection sensitivity by using at least four quantum states that can be easily attained by the contemporary technique.
CONSTITUTION: The phase modulation A which shows bits '0' and '1' with shift degrees 0 and π respectively or the modulation B which shows bits '0' and '1' with shift degrees $\pi/2$ and $-\pi/2$ respectively is added by a phase modulator 13 to a signal optical pulse 42 that is perfectly coincident with a reference optical pulse 41 in terms of their frequency and shapes. Thus a signal optical pulse 43 is acquired. Then the pulse 43 is transmitted together with the pulse 41, and the phase of a reference optical pulse 41a to be multiplexed with a received signal optical pulse 43' by a beam splitter 21 is shifted by 0 or $\pi/2$ by a phase modulator 23. Thus the measurement of the phase modulation A or B is selected, and the bit value of the pulse 43' is identified.



LEGAL STATUS

[Date of request for examination]	16.03.2000
[Date of sending the examiner's decision of rejection]	16.12.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平8－139701
(43)公開日　平成８年(1996)５月31日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｋ　1/00		Ｚ		

審査請求　未請求　請求項の数２　ＯＬ　（全 ９ 頁）

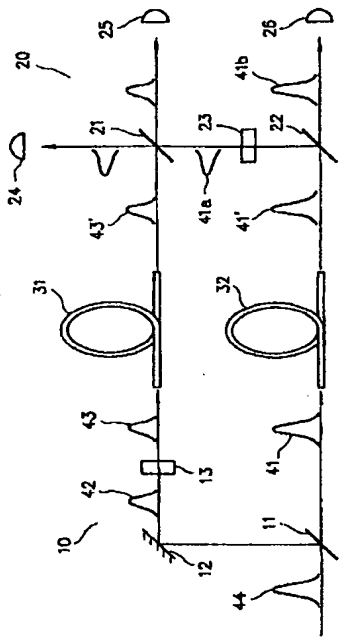
(21)出願番号　特願平6－280449

(22)出願日　平成６年(1994)11月15日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　井元　信之
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　吉田　精孝

(54)【発明の名称】　量子暗号方式

(57)【要約】
【目的】　現在の技術で容易に実現可能な少なくとも４つの量子状態を用いて盗聴検知の感度が高い量子暗号方式を提供する。
【構成】　周波数もパルスの形状も参照光パルス４１と完全に一致した信号光パルス４２に対し、位相変調器１３によりシフト量０でビット“０”を、シフト量πでビット“１”を表す位相変調Ａまたはシフト量π／２でビット“０”を、シフト量－π／２でビット“１”を表す位相変調Ｂを加えて信号光パルス４３となし、これを参照光パルス４１とともに送信し、受信された信号光パルス４３’にビームスプリッタ２１で合波する参照光パルス４１ａの位相を位相変調器２３により０またはπ／２ずらすことによって位相変調ＡまたはＢのいずれを測定するかを選択して信号光パルス４３’のビット値を識別する。



1

【特許請求の範囲】

【請求項1】　光または物質の量子状態のうち直交しない少なくとも2つの量子状態をそれぞれ有する複数のグループを用い、前記各グループのうちの一の量子状態でビット“0”を、他の量子状態でビット“1”を表し、送信側では複数のグループのうちのいずれのグループを用いるかを予め公開することなく送信し、
受信側では複数のグループのうちから一のグループをランダムに選び出して測定し、
測定終了後、送信側及び受信側が公開でグループ選択の一致・不一致及び受信側のビット識別の成功・不成功を確認することを特徴とする量子暗号方式。

【請求項2】　直交しない量子状態として位相が180度異なる一対のコヒーレント状態を用い、信号光のホモダイン検波によりこれらの量子状態を識別することを特徴とする請求項1記載の量子暗号方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、量子暗号、特に少なくとも4つの量子状態を備えた量子暗号を用いる暗号方式に関するものである。

【0002】

【従来の技術】暗号方式には、盗聴されていることを前提としてその解読が計算論的に困難であることを安全性の根拠に置く計算論的暗号方式（現代暗号とも呼ばれる。）と、量子力学の不確定性原理に基づいて盗聴者の有無をモニタしながら通信することを特徴とする量子暗号方式とがある。以下、従来の暗号方式及びその問題点について、計算論的暗号方式と量子暗号方式とに分けて述べる。

【0003】計算論的暗号方式については、
・池野信一、小山謙二　共著「現代暗号理論」（電子通信学会）
・岡本英司　著「暗号理論入門」（共立出版）
・今井秀樹　著「暗号のおはなし」（日本規格協会）
に詳しい解説があるが、大きく分けて秘密鍵暗号方式と公開鍵暗号方式に分けられる。

【0004】秘密鍵暗号方式の代表としてはIBM社より提案され米国商務省標準局（NBS）より1977年に公布されたDES（Data Encryption Standard）暗号方式があり、また、公開鍵暗号方式の代表としてはMITのRivest、Shamir、Adlemanにより発明されたRSA暗号方式がある。なお、量子暗号方式は秘密鍵暗号方式の一種と解釈される。

【0005】まず、計算論的暗号方式の代表としてDES暗号方式とRSA暗号方式の2つを取り上げる。

【0006】DES暗号方式とは、秘密鍵と呼ばれる共通の乱数例を送信者と受信者が事前に直接会う等の何らかの方法で安全に決定し（以後、このプロセスを「秘密鍵の決定」と呼ぶ。）、その後、交信すべきテキスト

2

（以後、平文と呼ぶ。）を秘密鍵の数列で決められる順序で転置と換字の処理を行うことにより暗号化及び復号を行う方式である。

【0007】現代では電子計算機を用いて処理するため、秘密鍵、平文、暗号化した文（以後、暗号文と呼ぶ。）のいずれも2進数列で扱う。秘密鍵の決定は経済的に高価につこうとも信頼性の高い通信（以後、秘匿通信と呼ぶ。）で行い、暗号文の交信には盗聴されても構わない廉価な通信（以後、公開通信と呼ぶ。）で行う。

【0008】一般に、秘密鍵暗号方式は事前に決定した秘密鍵を越える長さのテキストを送った場合、安全性が損なわれることが知られている。また、同じ秘密鍵を繰り返し使用した場合、試行錯誤的な秘密鍵の探索により解読される確率が大きくなる。従って、盗聴された暗号文が解読されないためには、頻繁に秘密鍵を変更し、その都度、高価な秘匿通信で秘密鍵の決定を行う必要がある。

【0009】秘匿通信としては、(1) 直接会う、(2) 完全に信頼できる第三者の媒介に頼る、(3) さらに安全な別の高級な暗号（例えば、量子暗号）を使う等が考えられる。なお、このような手段があるならば、これらを用いて直接、メッセージの交換を行えば良いように思われるが、そうしないのはメッセージの交換が必要となる事態は時間と場所を選ばず生じる可能性があるが、秘密鍵の決定は送信者と受信者の時間的都合が一致し、高価な方法を用いることができる場合を選んで行うことができるためである。このように、秘密鍵暗号方式の成否のポイントは秘密鍵の決定プロセスにあり、従来は安全な秘匿通信の実現が困難であった。

【0010】公開鍵暗号方式は前述した秘密鍵暗号方式における秘密鍵の決定プロセスを避けるために提案された暗号方式であり、秘匿通信を必要としない。その代表であるRSA暗号方式における手続きは次の通りである。

【0011】1．鍵生成プロセス：公開鍵と秘密鍵の生成を暗号受信者が行い、秘密鍵は自分で保持し、公開鍵は公開通信により暗号送信者に知らしめる。2つの大きな素数pとqを選び、その積$n=pq$を計算する。$(p-1)$と$(q-1)$の最小公倍数Lを計算し、Lと互いに素でLより小さな整数eを選ぶ。$ed \equiv 1 \pmod{L}$となるd、即ちLを法として$ed=1$となるdを求める。eとnが公開鍵、dが秘密鍵となる。

【0012】2．暗号化プロセス：暗号送信者が行う。平文を2進数の数Mとし、$C=M^e \bmod n$で定義されるCを暗号文とする。

【0013】3．復号プロセス：暗号受信者が行う。$M=C^d \bmod n$により平文Mを得る。

【0014】このように、手続きのどの段階においても秘匿通信が要求されない。この暗号を解読するためには公開鍵eとnから秘密鍵dを捜し当てる必要があるが、

そのためにはｎの因数分解ｎ＝ｐｑを求める必要がある。計算量理論から周知のように、整数の因数分解はＮＰ完全問題として知られ、ｎの桁数を大きくした時、計算量が指数関数的に増大する種類の問題である。例えば、ｎとして数百桁の整数を選ぶだけで、現代の最高速計算機を用いても、ｐとｑを捜し当てるのに数億年かかる。

【００１５】但し、これも周知のことであるが、因数分解の計算量が指数関数的に増大するのは現在、知られているアルゴリズムを用いた場合であって、どんなアルゴリズムを用いても計算量が指数関数的に増大することが証明されているわけではない。未知のアルゴリズムを用いた場合、その計算量が大幅に短縮される可能性が無いとはいえない。さらに、１９９４年５月に米国Santa Feで開催されたThird Santa Fe Workshop on Complexity, Entory and the Physics of Informationでは、量子チューリングマシン（量子計算機）を用いると因数分解の計算量が指数関数的ではなく多項式的程度で済むという証明がBell研究所から発表された。現在、量子チューリングマシンは実用化はおろか実験的にもまだ製作されていないが、今後、実験的研究段階に入る情勢にあることを考えると、ＲＳＡ暗号方式のような公開鍵暗号方式ももはや安全ではないという認識が暗号理論専門家の間に広まっている。

【００１６】一方、量子暗号方式を用いると、前述した問題点は克服される。これは秘密鍵暗号方式の一種であり、秘密鍵の決定を行う秘匿通信を量子力学的通信で行うものである。量子暗号方式については、

・Ａ．エカート　著／井元信之　訳「量子暗号理論への招待」パリティ、Vol.8, No.5, P.31, 1993

・Ｇ．コリンズ　著／井元信之　訳「量子暗号は史上最強の暗号」パリティ、Vol.7, No.2, p.26, 1992

に詳しい解説があるが、従来例として１９８４年にＩＢＭ社のベネット及びモントリオール大学のブラサールにより提案された方法を説明する。

【００１７】これは光子の偏光状態に“０”または“１”の１ビット情報を載せる方法で、２進数列は偏光状態が一つ一つ異なる光子列で表される。但し、偏光は直線偏光と円偏光の２種類を用い、直線偏光を使った場合は水平偏光を“０”、垂直偏光を“１”、円偏光を使った場合は右回り偏光を“０”、左回り偏光を“１”のように送信者と受信者との間で公開で取り決めておく。この量子暗号方式は一光子の４つの量子状態（水平、垂直、右回り、左回りの４偏光状態）を用いるので、４状態量子暗号方式と呼ばれる。

【００１８】秘密鍵の決定は、次に述べるように盗聴者の存在をモニタしつつ送信者及び受信者間で行われる。図２に以下のプロセスに対応した送受信のようすの一例を示す。なお、図中、

【外１】

は送信または受信における直線偏光の選択、

【外２】

は送信または受信における円偏光の選択、

【外３】

は水平直線偏光、

【外４】

は垂直直線偏光、「左」は左回り円偏光、「右」は右回り円偏光、「×」は捨てるビットを示している。

【００１９】(1) 送信者は２進乱数列を直線偏光または円偏光のいずれかを選択して変調する。どちらの偏光を用いるかは光子一つ一つについてランダムに選択し、選択の結果は受信者にも知らせずに送信する。

【００２０】(2) 受信者は送信者と独立に直線偏光か円偏光かのどちらかを選択して測定する（量子力学の原理により、一つの光子の直線偏光と円偏光とを同時に測定することはできないため）。その結果、得られたビット列のうち、およそ半分は直線偏光か円偏光かの選択が送信者及び受信者間で一致したビットとなり、この分については送信者のビットの値を受信者が正しく受け取る。残りの半分については両者の間で全く相関の無いビットの値になる。

【００２１】(3) 受信者の測定終了後（一連のビット全ての測定後でも１ビット毎の測定後でも良い。）、送信者と受信者は直線偏光または円偏光のいずれを選択したかを公開で照合する。

【００２２】(4) 選択が一致していないビットについては、前述のように送信者と受信者のビット間に全く相関がないので、送信者も受信者もそれらを棄却する。

【００２３】(5) 選択の一致したビットについては、盗聴が行われていない限り、後述のように送信者と受信者は同じビットの値を共有している。そのことを確認するために、いくつかのビットを間引いてテストビットとし、ビットの値を公開で照合する。

【００２４】(6) 十分多くのテストビットについて答が一致すれば、盗聴のないことが結論され、照合していない残りのビットは送信者と受信者で一致しており、かつ他の人物に知られていないことが保証される。これを秘密鍵として採用する。

【００２５】以上は盗聴されずに秘密鍵の決定が成功した場合であるが、盗聴が発見された場合、その量子通信路は安全でないので、盗聴が無いことが確認されるまで通信路を変更する等の措置をとり、前述した手続きを繰り返す。

5

【００２６】テストビットの値が異なった時、それが盗聴の結果であると結論される根拠は次の通りである。

【００２７】送信者も盗聴者もたまたま同じ偏光、例えば直線偏光を選択した場合、盗聴者は直線偏光の量子非破壊測定を行うか、全く同じ偏光状態の光子を再発生することができるので、盗聴を覚られない。しかしながら、盗聴者が送信者と異なる選択をした場合（このような確率は１／２であるが）、例えば送信者が直線偏光を、盗聴者が円偏光を選んだ場合、盗聴者は光子の偏光状態を直線偏光から円偏光に変えてしまう。そこで、受信者の測定結果が送信者と矛盾する場合がさらに確率１／２で生ずる。従って、盗聴が発覚しない確率は１ビットにつき１－１／２×１／２＝３／４となるので、ｎビットのテストビットを用いた場合、盗聴が発覚しない確率は（３／４）^{n}となる。従って、十分長いビット列を用いることにより、盗聴が発覚しない確率は桁数に対して指数関数的に任意の精度で０に近づけることができる。

【００２８】盗聴検出のために犠牲にするテストビットの割合は少なければ少ないほど良い。仮に、１０$^{-16}$の危険率（見逃す確率）で盗聴を検知したいとすれば１０$^{-16}$＝（３／４）^{n}より、テストビットとして必要なビット数ｎは約８０である。例えば、１００桁の秘密鍵生成の作業中に盗聴の有無をモニタしたいとすれば、その都度、８０桁のテストビットを犠牲にする必要がある。これでは鍵とテストビットの桁数がほぼ同じであるので、テストビットの割合を少なくするためには危険率をもっと高く設定し直すか、（３／４）^{n}より早く収束するような新たな量子暗号方式を開発する必要がある。

【００２９】このような量子暗号方式の優劣を比較する性能指数については後述するが、一般に、盗聴者に漏れた情報量と盗聴検知の感度との関係を比較するのが便利である。例えば、盗聴者に漏れる情報量が一定の条件の元に盗聴検知の感度が高い量子暗号方式が望まれる。

【００３０】前述した４状態量子暗号方式では、一つのパルスに１個の光子という規則的単光子列を制御性良く発生する技術があることを前提としているが、規則的単光子列発生は現在、実現されていないため、実験では通常のレーザで発生可能なコヒーレント状態と呼ばれる量子状態の光が用いられる。

【００３１】コヒーレント状態の光では一つのパルスに含まれる光子数の確率分布はポアソン分布となることが知られており、一パルスに１光子という規則性はない。しかしながら、コヒーレント光を十分減衰させることにより、一パルスに検出される平均の光子数が１より十分小さくなるようにできる。例えば、一パルス当たり平均０．１個の光子が含まれるようなコヒーレント光を用いた場合、およそ１０に一つのパルスが光子を１個だけ含む。この場合、規則的単光子列に比べて通信速度は約１／１０に落ちている。一つのパルスが光子を２個以上含

6

むこともあるが、これはおよそ２００に一つのパルスである。従って、光子を少なくとも１個含むパルスだけに着目すると、約２０に一つのパルスが光子を少なくとも２個含む。光子数が少なくとも２個のパルスについては、盗聴者は１光子のみを取り出して気づかれずに情報を盗聴することができるが、その頻度はこの例では１／２０であり、平均光子数を十分小さくすることにより、この頻度を任意の割合で小さくすることができる。

【００３２】しかしながら、コヒーレント光の使用を可能とする前述した議論が成立するのは通信路に光損失がない場合であり、光損失がある場合は以下に述べるようにコヒーレント光の使用は致命的欠陥をもたらす。

【００３３】即ち、現在の技術では石英光ファイバの最低損失値は０．２ｄＢ／ｋｍである。この光ファイバによる５０ｋｍの通信路を考えると、全体で１０ｄＢ、つまり９０％の損失となる。送信者が用いるコヒーレント光の平均光子数を、前述の例のように０．１とすると、このパルス列が１０ｄＢの損失を受けて受信者に到着した場合、受信者は平均して１００に一つのパルスで光子を検出可能となる。

【００３４】通信路に損失があること自体は量子暗号にとって致命的ではない。既に決まっているメッセージを送る通常の通信と異なり、量子暗号は秘密鍵を決定するプロセスであるから、損失により届かなかったビットは秘密鍵として採用されないだけのことである。問題は損失による光子の欠落なのか、盗聴による光子の欠落なのかを識別できない事態が生じ得ることにある。

【００３５】例えば、盗聴者が損失「０」の通信路を持っていて、この通信路で光ファイバを置き換えたとする。あるいは同じことであるが、盗聴者が送信者の送信直後に損失「０」で光子の偏光を測定し、その情報を元に受信者の直前で偏光した光子をいくつか再生し、送信者を装ったとする。この時、送信者及び受信者にとって、１０ｄＢの光子欠損がファイバの損失によるものか盗聴者の盗聴によるものか区別できない。これによる情報漏洩を見積ると次のようになる。

【００３６】前述のように２００の送信パルスのうちの一つは光子を２個含むので、そのパルスについては誤り発生なしに盗聴することができる。これは受信者が受信するパルスの頻度（１００に一つ）の半分に達する。即ち受信者が受信するパルスのうち半分は発覚することなく完全に盗聴され得ることになる。以上の数値例は一例であるが、定性的には一定値以上の通信速度及び一定値の光損失を前提とすれば、発覚することなく完全に盗聴されるパルスの頻度をある一定値以下に抑えることができないことは明らかである。

【００３７】

【発明が解決しようとする課題】従来技術とその問題点をまとめると、以下のようになる。計算論的暗号方式には秘密鍵暗号方式と公開鍵暗号方式の２種類がある。前

者は秘密鍵の安全な決定法がないという問題があり、後者は安全性の根拠である因数分解の計算量の発散性が証明されたものではなく、逆に量子チューリングマシンを用いれば発散しないことが証明されており、今では安全性の根拠が原理的には希薄になったと認識されている。量子暗号方式は盗聴がないことを確認しながら秘密鍵の決定を行う手段を与えるものであり、前記計算論的暗号方式の欠点を克服するものである。

【００３８】しかしながら、従来、提案された偏光を利用する４状態量子暗号方式では、第１に、テストビットの長さを秘密鍵そのものの長さと比べて大幅に短くすることはできない。第２に、現在、単光子パルス列を発生する技術がないので、通常のレーザ光と同じ性質のコヒーレント光パルスを用いざるを得ず、この場合、通信路の損失による情報損失と盗聴の区別がつかないことにより盗聴する自由度を盗聴者に与えてしまうという問題があった。

【００３９】本発明の目的は現在の技術で容易に実現可能な少なくとも４つの量子状態を用いて盗聴検知の感度が高い量子暗号方式を提供することにある。

【００４０】

【課題を解決するための手段】前記目的を達成するため、本発明では、光または物質の量子状態のうち直交しない少なくとも２つの量子状態をそれぞれ有する複数のグループを用い、前記各グループのうちの一の量子状態でビット“０”を、他の量子状態でビット“１”を表し、送信側では複数のグループのうちのいずれのグループを用いるかを予め公開することなく送信し、受信側では複数のグループのうちから一のグループをランダムに選び出して測定し、測定終了後、送信側及び受信側が公開でグループ選択の一致・不一致及び受信側のビット識別の成功・不成功を確認する量子暗号方式を提案する。

【００４１】

【作用】本発明によれば、送信側ではビット“０”及び“１”を、光または物質の量子状態のうち直交しない少なくとも２つの量子状態をそれぞれ有する複数のグループのうちのいずれかの一の量子状態及び他の量子状態を用いて送信し、受信側では任意のグループを選択して量子状態を測定し、その後、公開でグループ選択の一致・不一致及びビット識別の成功・不成功を確認することにより、ビット“０”及び“１”を確定する。

【００４２】

【実施例】図１は本発明の量子暗号方式の第１の実施例を示すもので、図中、１０は送信装置、２０は受信装置、３１，３２は光子通信路である。

【００４３】送信装置１０はビームスプリッタ１１、ミラー１２及び位相変調器１３を備えており、また、受信装置２０はビームスプリッタ２１，２２、位相変調器２３及びディテクタ２４，２５，２６を備えており、両者は光ファイバ等からなる光子通信路３１，３２により結ばれている。

【００４４】量子暗号方式の一般的前提として、送信装置は送信者の管理下に、受信装置は受信者の管理下にあり、その間の光子通信路は盗聴者が操作可能とする。送信者と受信者は意思を同じくし、盗聴者による通信路の操作がないことをモニタしながら秘密鍵の決定を行うことを目的とする。盗聴者は物理法則に反しない限り、どのような手段も使えることを前提とする。また、送信者と受信者は図１に示した装置以外に電話等の公開通信（電話自体は公開ではないが、盗聴監視や防止の手段を講じていないという意味で）の手段を持っており、この公開通信は盗聴されていることを前提とする。

【００４５】送信装置１０では参照光パルス４１を送信するとともに該参照光パルス４１の光学的位相を基準として信号光パルス４２の位相を変調し、信号光パルス４３として送信する。

【００４６】参照光パルス４１及び信号光パルス４２は周波数もパルスの形状も完全に一致している必要があるが、これは図示しない光源より発生した光パルス４４をビームスプリッタ１１で分けることにより実現できる。光パルス４４としては通常のレーザ光を変調して得られるパルス列やモードロックレーザのパルス列が用いられる。従って、光パルス４１，４２，４３，４４はいずれもコヒーレント状態にある。

【００４７】波長域の例としては現在、単一光子検出ＡＰＤ（アバランシェ・フォトダイオード）が利用可能な近赤外領域が考えられ、光パルス発生には化合物半導体レーザのパルス変調が用い得る。ビームスプリッタ１１の反射率を適当に選ぶことにより、また、必要に応じて光減衰器を用いることにより、信号光パルス４３は平均光子数が１以下の微弱光パルスとする。また、参照光パルス４１は平均光子数が最低約１０００の通常の光パルスにしておく。

【００４８】コヒーレント状態の光の光子数はポアソン分布を示し、平均Ｎのポアソン分布において光子数が０となる確率はe^{-N}であるから、平均光子数が１以下である信号光パルス４３に検出される光子数が０であることが頻繁に起こる。この光子を検出したりしなかったりする不確定さは、本発明において盗聴者にさらなる困難をもたらすが、それについては後述する。

【００４９】一方、参照光パルス４１の光子数が０となる確率はe^{-1000}であり、これは０と見なせる。光子数１０００以上の光パルスは光通信用のＡＰＤやＰＩＮフォトダイオードで確実に受信できる。受信装置のディテクタ２６としてはこのようなディテクタを用いる。

【００５０】送信装置１０ではビット情報“０”及び“１”を信号光パルス４２の位相にエンコードするが、従来の４状態量子暗号方式で直線偏光と円偏光の二種類の偏光変調を行った場合と全く同様に、本実施例では位相変調Ａと位相変調Ｂの二種類を用意する。位相変調Ａ

では位相シフト０をビット“０”に、位相シフトπをビット“１”に対応させ、位相変調Ｂでは位相シフトπ／２をビット“０”に、位相シフトπ／２をビット“１”に対応させる。位相シフトは位相変調器１３を用いて行うが、これは通常のポッケルスセルやカーセル等の市販の位相変調器で良い。

【００５１】信号光パルス４２の光の量子状態はコヒーレント状態なので、慣例に従ってこれを｜α〉と書くと、位相０，π／２，π／３，３π／２の変調を受けた後の状態は、それぞれ｜α〉，｜ｉα〉，｜－α〉，｜－ｉα〉となる。

【００５２】図３にビット“０”及び“１”をこれら４状態にエンコードする規則をまとめる。送信者はビット値はもちろん位相変調ペアＡまたはＢの選択も伏せて受信者へ向けて送信する。これはちょうど従来の量子暗号方式において直線偏光と円偏光のいずれを選んだかを伏せて送信するのと同じである。

【００５３】受信装置２０では到達した参照光パルス４１’の強度を反射率の低いビームスプリッタ２２により信号光のレベルまで大幅に落して参照光パルス４１ａとする。ビームスプリッタ２２を通過した残り大部分の参照光パルス４１ｂはディテクタ２６で検知され、ディテクタ２４，２５のトリガ用等に用いる。

【００５４】信号光と同じレベルになった参照光パルス４１ａをビームスプリッタ２１により信号光パルス４３’と干渉させる。ビームスプリッタ２１の透過率及び反射率を５０％とすれば、信号光パルス４３’と参照光パルス４１ａの相対位相が０の時は全ての光がディテクタ２５へ、また、πの時は全ての光がディテクタ２４へ行く。従って、参照光パルス４１ａの位相を位相変調器２３により０またはπ／２ずらしておくことにより、位相変調ペアＡを測定するかＢを測定するかの選択ができる。

【００５５】ディテクタ２４，２５としては単光子検出能力のあるディテクタが必要である。光子検出によく用いられる光電子増倍管（通称フォトマル）は速度が遅いことと量子効率が低いことから推奨されない。雑音が少なく長波長領域でも利用できる光検出デバイスとして最近、使われ始めている光子計数領域でのヴァキューム・アバランシェ・フォトダイオード等の半導体光子検出デバイスが現在のところ最適である。

【００５６】図４に受信者の選択と測定結果に基づく受信者のビット値の結論を示す。図ではディテクタ２４も２５もカウントなしという場合も想定されているが、これは信号光パルスの平均光子数が１より小さいために起こり得る。この場合、受信者はビット値の結論を出せないので、結論を“？”としておく。この“？”は従来の４状態量子暗号方式にはなく、本発明の特徴である。

【００５７】しかし、とりあえず“？”となる状況を無視してみると、容易に分かるように、本実施例の送受信の手続きは図２に示した従来方式の場合と同じであり、図２において

【数１】

⊕　―　位相変調Ａ

⊙　―　位相変調Ｂ

｜　―　｜α〉

―　―　｜－α〉

右　―　｜ｉα〉

左　―　｜－ｉα〉

と読み変えるだけで良い。このように“？”の存在を無視すれば、本発明は従来の４状態量子暗号方式において４つの偏光の変わりに｜α〉，｜ｉα〉，｜－α〉，｜－ｉα〉を用いたものに他ならない。

【００５８】なお、本実施例では参照光を光パルスとしたが、連続光としてもさしつかえない。この場合、ディテクタ２４，２５のトリガを別の信号で与える必要があるが、参照光と信号光との光路差をコヒーレント長以下にすれば良く、光路長の調整が容易になる。また、暗号の送信前に十分強い光信号を送信し、この光信号をもとに受信側で光ＰＬＬ回路等により局発光を生成しても良い。

【００５９】次に、前述した“？”の存在の利用法、即ち直交していない４つの量子状態を用いて４状態量子暗号を行う本発明方式を説明する。

【００６０】一般に、任意のコヒーレント状態が直交しないことは、関係式

$$|\langle\alpha|\beta\rangle|^2 = \exp(-|\alpha-\beta|^2)$$

からも明らかであるが、この式によれば、複素振幅αとβが複素平面上で遠いほど内積の絶対値は０に近づき直交性が増すが、近いほど１に近づいて直交性がなくなる。本実施例の｜α〉と｜－α〉もしくは｜ｉα〉と｜－ｉα〉の直交性はいずれも$\exp(-4|\alpha|^2)$となり、平均光子数が１より十分小さいコヒーレント状態光を用いた場合、特に直交性は低い。

【００６１】このような直交していない２つのベクトルを測定により識別することはできず、一般にはある確率で識別誤りを伴う測定しか実行できない。しかし、半確定的測定とも言うべき方法が存在する。

【００６２】これは直交していない２つの状態｜ϕ_1〉と｜ϕ_2〉についての測定の結果が(i)｜ϕ_2〉ではありえない、(ii)｜ϕ_1〉ではありえない、(iii)どちらとも言えない、という３種類の答を出力するような測定である。もし考えられる状態が｜ϕ_1〉と｜ϕ_2〉以外にない場合、これは(i)確実に｜ϕ_1〉である、(ii)確実に｜ϕ_2〉である、(iii)どちらともいえない、とい

う３種類の答を意味する。この場合、(i) または(ii)のケースを確定成功、(iii) を不成功ということにすれば、受信者は成功であったか不成功であったかを送信者に告げるだけで、(i) か(ii)かの情報は送信者と受信者の間で共有される。

【００６３】さて、このような非直交状態の測定を受信者が行う場合、図２で変更すべき点は、まず、ステップ(2) において受信者は全てのビットを受信できるわけではなく、いくつかは“？”、即ち“受信できなかった”とすべきビットがある。どのビットが受信できなかったかはステップ(3) において受信者から送信者に公開で通知することとする。即ちステップ(3) において選択の照合を行うだけでなく、半確定的測定の成功・不成功の情報も受信者から送信者に通知する。

【００６４】この場合に盗聴が発覚する可能性を考えてみる。盗聴者がたまたま送信者と同じ選択、例えば｜α〉と｜－α〉を識別する測定を選択したとする。この場合、従来方式では盗聴が発覚しなかったのであるが、本発明においてはこの場合も盗聴が発覚する可能性が生ずる。

【００６５】盗聴者が確定的測定に成功した場合は全く同一の量子状態にある光を再生し、送信者を装って確実に盗聴検知の網をくぐることができる。一方、確定的測定に成功せず“？”の結果を得た場合、とにかく｜α〉であったか｜－α〉であったかを推量して光の量子状態を作り、受信者に送る必要がある。そうしなければ遮断、即ち盗聴が発覚するからである。しかし、推量が誤りである確率が約１／２であるから、遮断した場合の発覚の確率を半分にできるに過ぎない。

【００６６】つまり本発明においては、従来方式におけるペア選択の誤りによる盗聴発覚の可能性に加えて、４状態が直交していないことによる確定的測定不成功の際の盗聴発覚の可能性が新たにつけ加わることになり、盗聴者にとっては困難が二重となる。

【００６７】以上は定性的な説明であるが、定量的には「盗聴検出感度ｐを一定とした時の盗聴者への漏洩情報量（シャノンの相互情報量）Ｉ＝Ｉ(p)」を用いて比較されるべきである。その計算は数値計算を必要とするので詳しい導出法は省略するが、通信速度ｒをパラメータとしてＩｒ(p)を計算することにより、全てのｒについて本実施例のＩｒ(p)は常に従来の４状態量子暗号方式のそれより小さいことが示される。特にｒが小さい極限では盗聴者と受信者との間の相互情報量は従来方式の半分となり、盗聴者と送信者との間の相互情報量は従来方式よりいくらかでも小さくできることが示される。

【００６８】従来方式のもう一つの問題は、規則的単光子列の代わりにコヒーレント状態を用いた場合、通信路に損失がある時はその損失が通信路本体のものか盗聴によるものか区別できないため、盗聴の機会を許すことにあった。この点についても本発明は従来方式より優位性

を有する。

【００６９】例えば、従来例で述べたのと同様に１０ｄＢ、即ち９０％の損失が通信路にあり、盗聴者は９０％の光全てを自分の管理下に置き、残り１０％を自分の無損失通信路を用いて受信者に送り、送信者を装うことができるものと仮定する。盗聴者の取るべき最も確実な方法は、前記９０％の量子状態をどこかに保持しておき、事後に送信者と受信者が公開通信でペアの選択を照合し合うのを待ち、送信者の選択したペアが判明した時点でその測定を行うことである。このような盗聴者の攻撃に対し、従来方式では送信者と受信者は無防備であった。

【００７０】しかし、本発明においては量子状態の非直交性のために盗聴者が確定的測定に成功する確率は低い。受信者が確定的測定に成功しなかったビットは捨てられて盗聴の意味がなくなるので、受信者が確定的結論を得たビットについて盗聴者も確定的測定に成功する必要があるが、受信者の確定的測定成功と盗聴者の成功は独立事象なので、この確率は直交性を小さく選ぶほど低くすることができる。

【００７１】図５は本発明の第２の実施例を示すもので、ここでは光子通信路の独立した２つの偏光モードを用いて１本の光子通信路で信号光及び参照光を伝送するようになした例を示す。即ち、図中、１４及び２７はそれぞれ送信装置１０及び受信装置２０に設けられた偏光ビームスプリッタであり、参照光パルス４１と信号光パルス４３を偏光ビームスプリッタ１５により独立した２つの偏光モードとして合波して光子通信路３１に送出し、偏光ビームスプリッタ２７で分離する如くなっている。また、１５，２８はミラーである。なお、その他の構成及び作用は第１の実施例の場合と同様である。

【００７２】図６は本発明の第３の実施例を示すもので、ここでは時間差を用いて１本の光子通信路で信号光及び参照光を伝送するようになした例を示す。即ち、図中、１６，２９はビームスプリッタであり、送信装置１０ではビームスプリッタ１１－１６間を直接結ぶ経路とミラー１２及び１５を介して結ぶ経路との光路差により参照光パルス４１と信号光パルス４３とに時間差を与えて光子通信路３１に送出し、受信装置２０ではビームスプリッタ２９－２１間を直接結ぶ経路とミラー２８及びビームスプリッタ２２を介して結ぶ経路との光路差により前記時間差を相殺して干渉させる如くなっている。なお、その他の構成及び作用は第１の実施例の場合と同様である。

【００７３】また、これまでは量子状態が４つの暗号について説明したが、量子状態が４以上の暗号に対しても本発明は適用できる。

【００７４】

【発明の効果】以上説明したように本発明によれば、直交しない少なくとも２つの量子状態をそれぞれ有する複数のグループを、現在の技術で容易に実現可能なコヒー

13

レント状態の光を用いて構成でき、また、各グループを構成する少なくとも２つの量子状態が直交しないことによる不確定性によって盗聴者に漏洩する情報量を従来方式に比べて格段に少なくする、言い替えれば同じ漏洩情報量であれば盗聴検知の感度を著しく高くすることができ、さらにまた、受信者と盗聴者とにおける前記不確定性の独立性により、通信路の損失による盗聴の成功確率を任意の割合で小さくすることができる。

【図面の簡単な説明】

【図１】本発明の量子暗号方式の第１の実施例を示す構成図

【図２】従来の量子暗号方式における秘密鍵の決定プロセスに対応した送受信のようすの一例を示す図

【図３】送信側におけるビット値と量子状態との対応規則の一例を示す図

14

＊【図４】受信側における測定結果とビット値との対応規則の一例を示す図

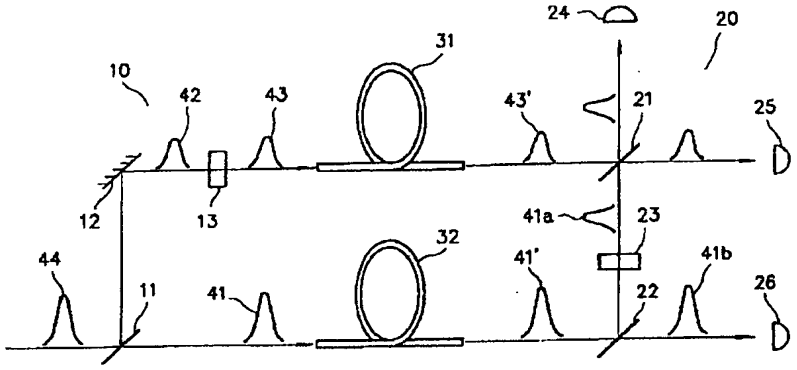
【図５】本発明の量子暗号方式の第２の実施例を示す構成図

【図６】本発明の量子暗号方式の第３の実施例を示す構成図

【符号の説明】

１０…送信装置、１１，１６…ビームスプリッタ、１２，１５…ミラー、１３…位相変調器、１４…偏光ビームスプリッタ、２０…受信装置、２１，２２，２９…ビームスプリッタ、２３…位相変調器、２４～２６…ディテクタ、２７…偏光ビームスプリッタ、２８…ミラー、３１，３２…光子通信路、４１，４１'，４１ａ，４１ｂ…参照光パルス、４２，４３，４３'…信号光パルス、４４…光パルス。

【図１】



【図２】

(1) 送信者の選択：	⊕	⊕	⊙	⊕	⊙	⊙	⊙	⊕	⊙	⊕	⊕	⊙	⊙	⊕	⊙	(非公開)
送った状態：	｜	―	右	｜	左	左	右	｜	左	―	｜	右	右	―	右	(非公開)
対応するビット：	1	0	1	1	0	0	1	1	0	0	1	1	1	0	1	(非公開)
(2) 受信者の選択：	⊕	⊗	⊕	⊕	⊗	⊗	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊕	⊗	(公開)
受信した状態：	｜	左	―	｜	左	左	｜	｜	左	―	左	右	―	―	右	(非公開)
対応するビット：	1	0	0	1	0	0	1	1	0	0	0	1	0	0	1	(非公開)
(3) 送信者は受信者の選択の正誤を公開：	正	誤	誤	正	正	正	誤	正	正	正	誤	正	誤	正	正	(公開)
(4) 生き残るビット																
送信者：	1	×	×	1	0	0	×	1	0	0	×	1	×	0	1	(非公開)
受信者：	1	×	×	1	0	0	×	1	0	0	×	1	×	0	1	(非公開)
(5) 送信者と受信者はビットを間引き公開照合	OK			OK				OK				OK				(公開)
(6) 照合後残るビット																
送信者：	×	×	×	1	×	0	×	1	0	×	×	1	×	×	1	(非公開)
受信者：	×	×	×	1	×	0	×	1	0	×	×	1	×	×	1	(非公開)
⇒ 秘密鍵				1		0		1	0			1			1	(非公開)

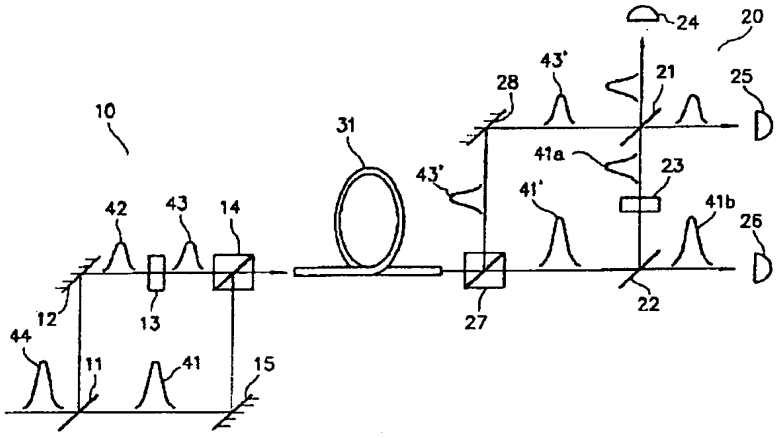
【図3】

ビット値	位相変調ペアの選択		位相シフト量	信号光状態
0	A	⇒	0	$\|\alpha\rangle$
	B	⇒	$\frac{\pi}{2}$	$\|i\alpha\rangle$
1	A	⇒	π	$\|-\alpha\rangle$
	B	⇒	$-\frac{\pi}{2}$	$\|-i\alpha\rangle$

【図4】

位相変調ペアの選択	ディテクタ25の出力	ディテクタ24の出力		保証される結論	ビット推定値
A	カウントあり	カウントなし	⇒	$\|-\alpha\rangle$ でない	0
	カウントなし	カウントあり	⇒	$\|\alpha\rangle$ でない	1
	カウントなし	カウントなし	⇒	何も言えない	?
B	カウントあり	カウントなし	⇒	$\|-i\alpha\rangle$ でない	0
	カウントなし	カウントあり	⇒	$\|i\alpha\rangle$ でない	1
	カウントなし	カウントなし	⇒	何も言えない	?

【図5】



【図6】